ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Cai, Yuanfeng; Zhu, Dan

Article

Fraud detections for online businesses: a perspective from blockchain technology

Financial Innovation

Provided in Cooperation with:
Springer Nature

Suggested Citation: Cai, Yuanfeng; Zhu, Dan (2016) : Fraud detections for online businesses: a perspective from blockchain technology, Financial Innovation, ISSN 2199-4730, Springer, Heidelberg, Vol. 2, Iss. 20, pp. 1-10, https://doi.org/10.1186/s40854-016-0039-4

This Version is available at:
https://hdl.handle.net/10419/176431

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

http://creativecommons.org/licenses/by/4.0/

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

Cai and Zhu *Financial Innovation* (2016) 2:20
DOI 10.1186/s40854-016-0039-4

Financial Innovation

RESEARCH Open Access

Fraud detections for online businesses: a perspective from blockchain technology

Yuanfeng Cai[1] and Dan Zhu[2*]

* Correspondence: dzhu@iastate.edu
[2]College of Business, Iowa State University, Ames, IA, USA
Full list of author information is available at the end of the article

Abstract

Background: The reputation system has been designed as an effective mechanism to reduce risks associated with online shopping for customers. However, it is vulnerable to rating fraud. Some raters may inject unfairly high or low ratings to the system so as to promote their own products or demote their competitors.

Method: This study explores the rating fraud by differentiating the subjective fraud from objective fraud. Then it discusses the effectiveness of blockchain technology in objective fraud and its limitation in subjective fraud, especially the rating fraud. Lastly, it systematically analyzes the robustness of blockchain-based reputation systems in each type of rating fraud.

Results: The detection of fraudulent raters is not easy since they can behave strategically to camouflage themselves. We explore the potential strengths and limitations of blockchain-based reputation systems under two attack goals: ballot-stuffing and bad-mouthing, and various attack models including constant attack, camouflage attack, whitewashing attack and sybil attack. Blockchain-based reputation systems are more robust against bad-mouthing than ballot-stuffing fraud.

Conclusions: Blockchain technology provides new opportunities for redesigning the reputation system. Blockchain systems are very effective in preventing objective information fraud, such as loan application fraud, where fraudulent information is fact-based. However, their effectiveness is limited in subjective information fraud, such as rating fraud, where the ground-truth is not easily validated. Blockchain systems are effective in preventing bad mouthing and whitewashing attack, but they are limited in detecting ballot-stuffing under sybil attack, constant attacks and camouflage attack.

Keywords: Blockchain, Fraud detection, Rating fraud, Reputation systems

Background

Nowadays the Internet permeates our daily lives. With the fast-growing information technology, the cyber world has transformed itself into a dominant platform, where people can exchange information, conduct business, and connect with others from all over the world. For example, Amazon had more than 285 million active users by 2015 (Lindner 2015). With the availability of unprecedented amounts of information, the Internet provides convenience to its users. Additionally, it produces challenges for users in processing information. Consequently, intelligent systems are widely applied to assist users in decision-making.

Springer Open

© The Author(s). 2016 **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

With built-in artificial intelligence in different knowledge domains, intelligent systems are capable of gathering information, processing problems, drawing inferences, and generating solutions (Krishnakumar 2003). Given input information and different built-in algorithms, intelligent systems can be applied to support decision making in various domains, such as finance, e-commerce, and healthcare. Regardless of the problem domain, the decision made by the intelligent system depends on users' inputs. Therefore, decision accuracy is vulnerable to fraudulent users' input, which is termed as information fraud. Unlike the real world, information in the cyber world is often input through a Web interface. With the advances in Web technology, users can inject fraudulent information easily, in various locations and without face-to-face interaction, making it both difficult and costly to detect fraud. As such, information fraud can hurt the effectiveness of intelligent systems, impair interaction trust in the cyber world, and result in financial losses.

Scholars have long examined information fraud. Since the built-in algorithms in intelligent systems are different, users also behave differently to inject fraudulent information. Consequently, various types of information fraud have been identified and summarized. Different supervised or unsupervised learning algorithms of fraud detection have been designed for each fraudulent scenario (Irissappane et al. 2012; Jøsang and Ismail 2002; Lee and Zhu 2012). Prior research has significantly improved the accuracy of information fraud detection; however, few models can maintain perfect detection performance in all fraudulent scenarios. Additionally, even if the fraudulent input is successfully identified, we may still not be able to access the truth and make the right decision. Furthermore, there are various reasons behind information fraud, such as concerns for personal privacy or seeking inappropriate profits (Lam and Ried 2004; Metzger 2004). The current detection algorithms cannot completely eliminate such behaviors.

In the era of decentralized computing, a breakthrough in blockchain technology, which underlines Bitcoin (Nakamoto 2008), can be used to preserve users' privacy and prevent information fraud. Blockchain is a public ledger that verifies every transaction, stores it based on group consensus, and records it indisputably (Soska and Christin 2015; Vandervort 2014). As it can provide transaction records permanently, incorruptibly, and irreversibly, it may help fundamentally prevent some types of information fraud (Khan 2015, Pwc 2015). In this paper, we analyze the effectiveness of blockchain technology in fraud detection. While there are various types of information fraud, in this study, we focus on one popular type: rating fraud. We consider a piece of information fraudulent as long as it is not consistent with real information.

In the subsequent section, we provide a brief introduction of rating fraud, followed by an overview of the literature on blockchain technology in An overview of blockchain technology section. In Effectiveness of Blockchain on Rating Fraud section, we discuss the effectiveness of blockchain technology on rating fraud. We conclude the paper in Conclusions and Discussion section with discussions.

An introduction to rating fraud

Online interactions with anonymous users can involve risks. In the real world, we can obtain feedback about a seller from previous customers before making a purchase. As such, people tend to purchase from highly reputed sellers, since purchasing products

from an unreliable seller may result in severe losses. Similarly, in the cyber world, we prefer to pre-evaluate the trustworthiness of a potential seller with support from reputation systems, as they are designed to help people to judge the quality of unknown vendors beforehand.

Reputation systems collect, aggregate, and distribute feedback about entities' past behaviors (Resnick et al. 2000). Theoretically, reputation is a distribution of opinions, estimations, or evaluations about an entity in an interest group (Bromley 2001). An interest group is one where the people within a group have some relationship or concern with an entity (Bromley 2001). Reputation systems have been validated as highly effective ways to protect customers from transactional risks. Numerous studies have shown that reputation systems are effective to reduce transitional losses, improve customers' buying confidence, help them make purchase decisions, and drive sales growth for sellers (Ba and Pavlou 2002; Bolton et al. 2004; Park et al. 2007). Despite their effectiveness, they are vulnerable to rating fraud, a phenomenon wherein raters benefit themselves by creating biased ratings (Cai and Zhu 2015; Mayzlin et al. 2014). Rating fraud is common in the cyber world, and some companies commit such activities. For instance, 19 review management companies were caught and fined because of injecting dishonest ratings into various sites, such as Yelp.com (Sved 2014).

In the cyber world, there are two types of measures for rating: non-computational and computational (Zacharia et al. 2000). A non-computational rating is not a numerical value; instead, it keeps a record of all the activities associated with that evaluation. A famous example of a non-computational rating system is the Better Business Bureau Online, whose primary responsibilities are handling disputes and tracking complaints (Azari et al. 2003). In contrast, a computational rating is calculated based on the evaluations from all evaluators. For the computational rating, there are two types of rating systems: content-and user-driven. Content-driven systems (i.e., WikiTrust) use automated content analysis to derive ratings by comparing contributed content with the truth. The content is more reliable if it is less frequently modified. However, there are several limitations to content-driven rating systems. The ratings are calculated automatically and are nontransparent to users; therefore, the users' belief in rating scores is affected as they do not understand the internal calculation process. Additionally, such systems rely on raters' proactive content verification. If users do not provide feedback, rating reliability becomes misleading.

User-driven ratings systems (i.e., eBay or Amazon) compute their rating scores based on users' rating. In user-driven rating systems, the rating score can be calculated either as the difference between all positive and negative scores (e.g., eBay) (Resnick and Zeckhauser 2002), or as the average of all ratings (e.g., Amazon) (Schneider et al. 2000). In a more advanced version, it can utilize the previous positive and negative ratings as parameters to formulate the beta probability density function of each rating. For example, in beta reputation systems, given the previous rating score and the new rating, the updated one can be calculated (Jøsang and Ismail 2002).

In user-driven rating systems, dishonest raters may have different goals; thus, they behave differently. For example, the incentives of fraudulent raters can either be promoting their own product or demoting their competitors'. According to Dellarocas (2000), unfairly high ratings injected by fraudulent raters to a target entity are termed as "ballot stuffing," and the unfairly low ratings are called "bad mouthing."

Regardless of bad mouthing or ballot stuffing, we follow six types of fraudulent raters' behavior models summarized in Irissappane et al. (2012). The first three are "constant attack," "camouflage attack," and "whitewashing attack." A "constant attack" indicates that a fraudulent rater consistently provides unfairly high (low) ratings to the target entity in a ballot stuffing (bad mouthing) scheme. A "camouflage attack" is performed by a strategical fraudulent rater, who will inject fair ratings to non-target entities to camouflage himself/herself, in addition to injecting unfair ratings to the target entities. This type of attack brings more challenges to the reliability of reputation systems, as it is more difficult to differentiate fraudulent raters from honest ones because their ratings are more similar to each other. In a "whitewashing attack," a rater will inject unfair ratings to the target entity for a period. Subsequently, he/she whitewashes himself/herself by creating a new account and thereupon behaving as an honest rater.

Each of these three types of attacks can be used to commit either a ballot stuffing or bad mouthing scheme, with the only difference being the rating value (i.e., unfairly high or unfairly low) of the target entity. In addition to the abovementioned attack types, Douceur (2002) proposes the concept of the "Sybil Attack." Different from the previous three types of attack models, it does not regulate the fraudulent rater's behavior, but describes the overall fraudulent population. When there are more dishonest raters than honest ones in the system, the system is under a sybil attack. This can be combined with the three types of fraudulent behaviors, namely constant, camouflage, and whitewashing, resulting in a "sybil constant attack," "sybil camouflage attack," or a "sybil whitewashing attack," respectively, wherein each one indicates that in the reputation system, there are fewer honest raters than fraudulent ones.

An overview of blockchain technology

Blockchain is built on the Bitcoin protocol, the first peer-to-peer (P2P) electronic case systems that allow payments to be sent online from one entity to another without the intervention of a financial institution (Nakamoto 2008). As a result, trust is established not by powerful intermediaries, such as banks, governments, and technology companies, but through mass collaboration and clever code on the Blockchain (Tapscott and Tapscott 2016). Blockchain is a transaction database shared by anyone participating in the system. With cryptocurrency, transactions records are stored as data blocks, which are chained together cryptographically. It is open to any node in the system and everyone can enter new entries. However, new blocks cannot be added without the proof-of-work and agreement by the other nodes participating in the system. Hereby, blockchain guarantees the accuracy of the information it stores. Blockchain is immutable; therefore, once a block is modified, it will also regenerate every subsequent block (Khan 2015).

The mechanism of blockchain technology can be explained from its first application. Bitcoin, a form of digital cryptocurrency, is different from the traditional currency issued by governmental financial institutions. Bitcoin is a ledger, storing account information and their balance, which works as an online bank account that every user can access, receive, and transfer money. This is different from a traditional bank, wherein the information is controlled by the central authority. The ledger of Bitcoin is owned by everyone in the Bitcoin network.

While the information is open to any code, information security is guaranteed by using one half of a digital signature (Elliptic Curve Digital Signature Algorithm). Each owner of the account holds and keeps half of the digital signature to himself/herself, which is called a "private key"; the other half of the digital signature, which is called a "public key," is published to all participants in the network. Each account owner can send bitcoins to the public key and use it to verify the accuracy of the signature; however, only the owner with the private key can use the bitcoins from the account. To send bitcoins, an account owner broadcasts the "sending-money" notification so that all participants in the network are notified; then the network validates the account information against its key. As the account balance will go down, the account owner needs to ensure that the account has sufficient balance; subsequently, a transaction will be made with the receiver's account and the balance will be adjusted accordingly. All nodes in the Bitcoin network will be notified about this transaction, and each node will include it and pass it on to other nodes. Once a transaction is included in a block, it becomes certified. Finally, every node on the Bitcoin network will have the same copy of the entire ledger. Therefore, instead of using a bank's network, a group of computers keeps a ledger.

In traditional banking systems, each customer is authorized solely to his/her own account information by using a pair of user name and password; however, in the Bitcoin network, every account is kept as a copy in each node. Therefore, the Bitcoin network needs to ensure that each transaction update is authentic; as a result, the digital signature is required for every transaction (Driscoll 2013). Whenever an account owner needs to initiate a transaction, he/she needs his/her private key to sign the transaction. Other participants can use the public key to verify the validity of this new transaction. If authentication is completed without any problems, a new digital signature will be added to the Bitcoin transaction, which can be completed only by its new owner. Other participants work independently on their own copy of the blockchain so as to ensure that the digital signature is incorruptible and the sender account has sufficient balance. A verified record is added to the block and is irreversible (Peck 2015).

Therefore, in essence, the blockchain is a recordkeeping technology, where each transaction is interlinked with an earlier record in the chain. This arrangement only converges if all participants agree on what should be the most recent version of the blockchain (Peck 2015). As it requires group consensus, the process to add new transactions into the blockchain is both complex and costly. A large amount of computation, which uses hash functions, is required from every node to verify and accept the new record. Thus, once the transaction is included, it is verified and not easily changed. Thus, transactions in the blockchain network seldom go backwards. Transactions entered into the blockchain ledger are secure; as such, they are described as permanent, incorruptible, and irreversible records (Khan 2015).

Blockchain system can be applied in various problematic domains. As all transactions must be publicly broadcasted and permanent, it can provide various types of services, such as delivery verification in the supply chain industry, degree verification in the educational industry, money transfer security in the financial industry, and payment chargeback risks mitigation in e-commerce (Khan 2015). Another important application area for blockchain systems is financial fraud detection. To facilitate business decision making, a variety of systems have been developed for processing applications.

Given the information provided by users, a decision is made based on the built-in decision rules. Such systems significantly improve the effectiveness and efficiency of application decision making, although they are vulnerable to manipulated input information, such as loan fraud.

For example, a decision on a loan application can be generated based on inputs of customers' personal information. When a user intends to apply for a loan through an online application system, he/she may falsify some of the personal financial information, such as a fake repayment history, thus increasing the possibility of acceptance. Consequently, financial institutions have suffered tremendous losses due to loan fraud (Kim et al. 2012). As blockchain systems can keep historical transactions records, applicants cannot falsify information to obtain a favorable decision. Among all the application areas, we focus on the applications on rating fraud detection in the subsequent section.

Effectiveness of blockchain on rating fraud

Recently, scholars have been focusing on redesigning reputation systems in the era of blockchain technology. For instance, Vandervort (2014) discusses the feasibility and challenges of designing the bitcoin-based reputation systems. As privacy is an important concern for users who are reluctant to provide information, Schaub et al. (2016) propose how to utilize digital signatures to design reputation systems that can protect users' privacy. In a similar vein, Soska and Christin (2015) propose a system "Beaver," which protects users' privacy, while being resistant against sybil attacks by charging fees. Dennis and Owenson (2016) design reputation systems with underlying blockchain technology. These systems generate and broadcast a binary P2P rating on receiving the correct file.

As discussed in Background section, privacy concerns drive users to contribute fraudulent information. With support from blockchain technology, Schaub et al. (2016) propose that customers and sellers use private and public keys to communicate with each other. Customers can be assigned tokens from sellers to be allowed to provide feedback. However, the rating can be unlined from customers. Therefore, customers do not need to worry about retaliation, and can provide real feedback.

In addition to privacy concerns, another important reason for rating fraud is seeking inappropriate profits. In the financial application fraud discussed in An overview of blockchain technology section, the fraudulent information is objective in that it is fact-based and provable. Thus, the ground truth of the fraudulent information can be assessed. As regards rating fraud, if it occurs in non-computational reputation systems and content-driven reputation systems, since the rating information is also fact-based, blockchain systems can be utilized to verify the validity of claims and content. However, for the rating fraud in user-driven reputation systems, the information is subjective in that it lacks ground truth. For example, even if an attacker demotes a decent item by injecting a poor rating, he/she can always insist that it is based on difference in individual preference. Therefore, even with accurate historical transactional records, it is still difficult to detect fraud on subjective information. In the method developed by Dennis and Owenson (2016), they propose that human opinions are removed from reputation systems. Instead, the reputation is represented by a binary value, which reflects if the file is received by the users. In this case, the systems contain only objective information,

which is fact-based. As such, blockchain technology can be used to support fraud detection. However, the purpose of reputation systems is to help users better understand sellers. If we only record whether the requested product is delivered, it does not satisfy all customers' needs. Product delivery is an important aspect of a seller; however, there are many other factors, such as product quality, which are also very important to customers' purchasing decisions.

Other studies on blockchain-based reputation systems, such as Soska and Christin (2015), propose a preventative mechanism against subjective information fraud, which is increasing the fees of injecting ratings. Such a preventive strategy has already been proposed in rating fraud for traditional reputation systems. For example, we can bind each account to one unique IP address to prevent a sybil attack (Douceur 2002). SybilGuard, a protocol proposed by Yu et al. (2006) is designed to increase the difficulty of controlling multiple accounts to perform the attack. In a similar vein, Epinions.com encourages raters to provide honest feedback by sharing income with them (Jøsang and Ismail 2002). The preventive mechanism increases the costs of fraud, so that it can mitigate sybil attacks. However, they are not effective if the perceived benefit from attacks is greater than the cost.

In traditional reputation systems, such as Amazon.com and Expedia.com, rating fraud can be dealt with by using the label "verified transaction." For example, Expedia raters must be real customers, i.e., who have checked in a hotel for at least one night (Mayzlin et al. 2014). Thus, ratings on Expedia are claimed as "verified ratings." Similarly, Amazon.com labels the rating if it is from a "verified purchase." With the support of blockchain technology, it is much easier to identify if the rating is from a valid purchase. Therefore, in blockchain-based reputation systems, only verified transactions and their associated ratings will be stored, making "verified" labels no longer necessary.

The immutable transactional records in blockchain-based reputation systems can be used to prevent some types of rating fraud. Schaub et al. (2016) suggest that bad mouthing, including sybil and non-sybil attacks, can be mitigated if a user can only rate a product after receiving a token from the seller. In such a scenario, every submitted rating must come from a transaction. Limiting ratings only to those with valid transactions significantly decreases the motivation of bad mouthing. This means that, if one company intends to demote its competitor's product, it first needs to contribute toward the competitor's sales. However, this is unlikely under a sybil attack, wherein more than half of the transactions are completed by fraudulent customers assigned by the competitors. Although it cannot rule out bad mouthing completely, if the perceived benefit is greater than the cost, a company needs strategically analyze how many resources it should devote to the fraud.

The effectiveness of blockchain-based reputation systems may be limited in ballot stuffing sybil attacks. The seller is likely to promote his/her own product by encouraging fraudulent raters to complete real transactions. Raters may be offered free or significantly discounted products so as to inject a positive review. This phenomenon has already been noticed by Amazon.com. Amazon has removed "verified purchase" badges from reviews associated with discounted transactions (Coleman 2016). The blockchain-based reputation systems can reflect such discounted transactions accurately, but are less effective in stopping their occurrence. Furthermore, sellers can allow customers to first pay the full amount, submit ratings, and pay them back in other

ways. Although transaction records are incorruptible in the blockchain-based reputation systems, the fraudulent raters in such false "real transactions" are not detected.

A strategy proposed by Schaub et al. (2016) to prevent ballot stuffing is limiting the total number of tokens for each seller. Therefore, if a seller gives tokens to fraudulent ratings, it will reduce the number of real transactions. This strategy is effective as it can result in a tradeoff between rating and profit for the seller. The assumption underlying this strategy is that the total size of ratings is limited. The purpose of reputation systems is to encourage users to provide feedback, and there is a natural difference between the rates of submission of products' ratings, e.g., "hit" products can receive more feedback within a shorter period, while unpopular products may not be commented on by customers for a long time. Consequently, it may not be feasible to limit the number of ratings that can be received from the start.

As regards ballot stuffing, constant and camouflage attacks, such subjective information fraud can be mitigated; although, it is difficult to prevent or detect them in blockchain-based reputation systems due to the existence of false "real transactions." However, blockchain technology can be used against whitewashing attacks. In the blockchain-based reputation systems, the user account can be created with real identity, while the real identity is not disclosed. Therefore, once a rater has injected fraudulent subjective information, he/she can leave the system, but he/she cannot create a new account so as to whitewash his/her past rating history.

Conclusions and discussion

Interactions in the cyber world are characterized by anonymity, which can occur between people who do not know each other's real identity. However, it may be risky to interact with unfamiliar items or unknown sellers in the cyber world. Rating systems have been shown to be effective for customers to pre-evaluate the quality of the object and control interaction-specific risks. However, rating systems are vulnerable to rating fraud, which may mislead the customers' purchasing decisions and further affect their motivation for future interaction. Blockchain is a distributed public ledger, which keeps records on thousands of computers. All records stored in the system are entered with proof-of-work, based on group consensus, and cannot be tampered with. Therefore, the true records in blockchain systems can be used to address the integrity issue.

This study discusses the potential strengths and limitations of blockchain-based reputation systems under rating fraud. Blockchain systems are very effective in preventing objective information fraud, such as loan application fraud, where fraudulent information is fact-based. However, for subjective information fraud, such as rating fraud, where the fraudulent information is not easily verified, blockchain systems are not effective in all scenarios. On one hand, blockchain technology is effective in preserving customers' privacy. Users may be reluctant to provide true information to reputation systems because of personal privacy concerns. As such, blockchain systems can prevent fraudulent ratings submitted by such users, as their real identify will not be disclosed. On the other hand, users may inject fake information into systems to promote their own products or demote their competitors' products. Blockchain systems are effective in preventing some types of rating fraud, such as bad mouthing and whitewashing attacks, but they may be unable to prevent ballot stuffing sybil, constant, and camouflage attacks.

The limitation that ratings can only be submitted after completing transactions increases the cost of rating fraud. However, sellers can still enter into agreements with raters for incentivized ratings. Fraudulent raters can submit unfair higher ratings in exchange for significantly discounted products or services, or they can complete the transaction, submit the rating, and be subsequently reimbursed by the seller. In such cases, blockchain systems keep accurate transactional information; however, they cannot verify whether the ratings are fraudulent or not as they are based on individual subjective evaluation. Additionally, we should be aware that blockchain systems are not perfect regarding information security. Although it is a recordkeeping technology that stores permanent and incorruptible records, it may not always guarantee the reliability. For example, blockchain systems can be utilized by some sophisticated hackers to inject malicious nodes and spread viruses. As all computers keep the same copy, a larger number of computers will be infected. In addition, Lemieux (2016) discusses practical issues for record reliability in blockchain-based solutions.

However, as users' privacy can be protected in blockchain systems, we can only allow accounts created using real identities to submit ratings. Compared to the traditional reputation systems wherein one person can control multiple account IDs and inject fake ratings, blockchain reputation systems can significantly decrease the number of fraudulent ratings. Future research lie in deep understanding of blockchain technology and development of new technologies in detecting both objective as well as subjective information frauds.

Acknowledgements
We would like to thank the anonymous reviewers for their constructive suggestions and comments that help to improve this manuscript.

Author's contributions
Both authors developed the central idea and contributed to the conceptualization of the study. All authors read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Zicklin School of Business, Baruch College, City University of New York, New York, NY, USA. [2]College of Business, Iowa State University, Ames, IA, USA.

Received: 12 November 2016 Accepted: 24 November 2016
Published online: 06 December 2016

References

Azari R et al (2003) Current security management & ethical issues of information technology. Idea Group Publishing, Hershey
Ba S, Pavlou P (2002) Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior. MIS Q 26(3):243–268
Bolton GE, Katok E, Ockenfels A (2004) How effective are electronic reputation mechanisms? An exp invest Manag Sci 50(11):1587–1602
Bromley DB (2001) Relationships between personal and corporate reputation. Eur J Mark 35(3):316–334
Cai Y, Zhu D (2015) Rating fraud detection—towards designing a trustworthy reputation systems. Proceeding of 36th International Conference on Information Systems (ICIS '15, Dallas, TX
Coleman A. (2016) Amazon banned incentivized reviews: Companies say reviews anyway. http://www.inquisitr.com/3568728/amazon-bans-incentivized-reviews-companies-say-review-anyway/. Accessed 1 Nov 2016
Dellarocas C (2000) Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. Proceedings of the 2nd ACM Conference on Electronic commerce. October 17-20, 2000, Minneapolis, Minnesota, pp. 150–157
Dennis R, Owenson G (2016) Rep on the roll: a peer to peer reputation system based on a rolling blockchain. Int J Digital Society (IJDS) 7(1):1123–1134
Driscoll S (2013) "How Bitcoin Works under the Hood," in: ImponderableThings. Blogger. http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Douceur J (2002) "The Sybil Attack," In IPTPS'01 Revised Papers from the First International Workshop on Peer-to-Peer Systems, Springer-Verlag London, UK 2002, pp. 251–260
Irissappane, A. A., Jiang S., & Zhang, J. (2012). Towards a Comprehensive Testbed to Evaluate the Robustness of Reputation Systems against Unfair Rating Attacks. UMAP Workshops, volume 872 of CEUR Workshop Proceedings.
Jøsang A, Ismail R (2002) The beta reputation system, in proceedings of the 15th bled electronic commerce conference
Khan A (2015) Bitcoin - payment method or fraud prevention tool? Comp Fraud Security. Volume 2015, Issue 5, May 2015, Pages 16–19
Kim J, Choi K, Kim G, Suh Y (2012) Classification cost: An empirical comparison among traditional classifier, cost-sensitive classifier, and metacost. Expert Syst with Appl 39(4):4013–4019
Krishnakumar K (2003) Intelligent Systems for Aerospace Engineering - An Overview., NASA Technical Report, Document ID: 20030105746
Lam S, Ried J (2004) Shilling recommender systems for fun and profi. 13th Internat. WWW Conf., ACM, New York, pp 309–402
Lee J, Zhu D (2012) Shilling attack detection—a new approach for a trustworthy recommender system. INFORMS J Comput 24(1):117–131
Lemieux V (2016) Trusting records: is Blockchain technology the answer? Rec Manag J 26(2):110–139
Lindner MV (2015) Amazon's rising tide lifts marketplace sellers. https://www.internetretailer.com/2015/07/24/amazons-rising-tide-lifts-marketplace-sellers. Accessed 1 Nov 2016
Mayzlin D, Dover Y, Chevalier J (2014) Promotional reviews: an empirical investigation of online review manipulation. Am Econ Rev 104(8):2421–55
Metzger MJ (2004) "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," J Comput Mediated Commun (9:4) 00
Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system., https://bitcoin.org/bitcoin.pdf
Park DH, Lee J, Han I (2007) The effect of on-line consumer reviews on consumer purchasing intention: the moderating role of involvement. Int J Electron Commer 11(4):125–148
Peck M (2015) "The Future of the Web Looks a Lot Like Bitcoin," Spectrum IEEE (1 July). http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin
PwC (2015) Information security breaches survey. Published in March 2015 by PWC in association with InfoSecurity Europe. https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf. Accessed 1 Nov 2016
Resnick P, Kuwabara K, Zeckhauser R, Friedman E (2000) Reputation systems. Commun ACM 43(12):45–48
Resnick, P., & Zeckhauser, R. (2002). Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. In M. R. Baye, editor, The Economics of the Internet and E-Commerce, volume 11 of Advances in Applied Microeconomics. Amsterdam, Elsevier Science. pp. 127–157
Schaub, A., Bazin, R., Hasan. O., & Brunie, L (2016) A trustless privacy preserving reputation system," in 31st IFIP TC 11 International Conference, SEC 2016, Ghent, Belgium, May 30 - June 1, 2016
Schneider J et al (2000) Disseminating trust information in wearable communities. Proceedings of the 2nd International Symposium on Handheld and Ubiquitous Computing (HUC2K, Bristol, UK
Sved D (2014) Nineteen companies found guilty of writing fake consumer reviews., http://www.heralddeparis.com/nineteen-companies-found-guilty-of-writing-fake-consumer-reviews/232920
Soska K, Christin N (2015) 'Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In: Proceedings of the 24th USENIX security symposium (USENIX Security'15., pp 33–48, As of 23 June 2016
Tapscott D, & Tapscott A (2016) "The Impact of the Blockchain Goes Beyond Financial Services," Harvard Business Review. https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services
Vandervort D (2014) Challenges and Opportunities Associated with a Bitcoin-Based Transaction Rating System. In Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados,March 3–7, 2014. pp, 33–42, Springer, Berlin, Germany
Yu H, Kaminsky M, Gibbons PB, Flaxman A (2006) SybilGuard: defending against Sybil attacks via social networks. In: Proceedings of the 2006 conference on applications, technologies, architectures, and protocols for computer communications. ACM Press, New York, pp 267–278
Zacharia G, Moukas A, Maes P (2000) Collaborative reputation mechanisms for electronic marketplaces. Decis Support Syst 29(4):371–388

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Immediate publication on acceptance
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com